الاتحـــــــــاد الدولـــــــــي للاتصـــــــــالات

ITU-T X.1253

(2011/09)

قطـــاع تقييس الاتصـــالات
في الاتحاد الدولي للاتصالات

السلسلة X: شبكات البيانات والاتصالات
بين الأنظمة المفتوحة ومسائل الأمن

أمن الفضاء السيبراني – إدارة الهوية

مبادئ توجيهية بشأن أمن أنظمة إدارة الهوية

التوصيـــة ITU-T X.1253

الاتحاد الدولي للاتصالات

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

الشبكات العمومية للبيانات	X.199–X.1
التوصيل البيني للأنظمة المفتوحة	X.299–X.200
التشغيل البيني للشبكات	X.399–X.300
أنظمة معالجة الرسائل	X.499–X.400
الدليل	X.599–X.500
التشغيل البيني لأنظمة التوصيل OSI ومظاهر النظام	X.699–X.600
إدارة التوصيل البيني للأنظمة المفتوحة (OSI)	X.799–X.700
الأمن	X.849–X.800
تطبيقات التوصيل البيني للأنظمة المفتوحة (OSI)	X.899–X.850
المعالجة الموزعة المفتوحة	X.999–X.900
أمن المعلومات والشبكات	
الجوانب العامة للأمن	X.1029–X.1000
أمن الشبكة	X.1049–X.1030
إدارة الأمن	X.1069–X.1050
الخصائص البيومترية	X.1099–X.1080
تطبيقات وخدمات آمنة	
أمن البث المتعدد	X.1109–X.1100
أمن الشبكة المحلية	X.1119–X.1110
أمن الخدمات المتنقلة	X.1139–X.1120
أمن الويب	X.1149–X.1140
بروتوكولات الأمن	X.1159–X.1150
الأمن بين جهتين نظيرتين	X.1169–X.1160
أمن معرفات الهوية عبر الشبكات	X.1179–X.1170
أمن التلفزيون القائم على بروتوكول الإنترنت	X.1199–X.1180
أمن الفضاء السيبراني	
الأمن السيبراني	X.1229–X.1200
مكافحة الرسائل الاقتحامية	X.1249–X.1230
إدارة الهوية	**X.1279–X.1250**
تطبيقات وخدمات آمنة	
اتصالات الطوارئ	X.1309-X.1300
أمن شبكات المحاسيس واسعة الانتشار	X.1339–X.1310
تبادل معلومات الأمن السيبراني	
نظرة عامة على الأمن السيبراني	X.1519–X.1500
تبادل مواطن الضعف/الحالة	X.1539–X.1520
تبادل الأحداث/الأحداث العارضة/المعلومات الحدسية	X.1549–X.1540
تبادل السياسات	X.1559–X.1550
طلب المعلومات الحدسية والمعلومات الأخرى	X.1569–X.1560
تعرف الهوية والاكتشاف	X.1579–X.1570
التبادل المضمون	X.1589–X.1580

لمزيد من التفاصيل، يرجى الرجوع إلى قائمة التوصيات الصادرة عن قطاع تقييس الاتصالات.

التوصيـــة ITU-T X.1253

مبادئ توجيهية بشأن أمن أنظمة إدارة الهوية

ملخص

تقترح التوصية ITU-T X.1253 مبادئ توجيهية بشأن الأمن من أجل أنظمة إدارة الهوية (IdM). وتوضح هذه المبادئ التوجيهية الكيفية التي ينبغي لأنظمة إدارة الهوية أن تنشر وتشغل بها من أجل تقديم خدمات هوية آمنة في بيئة شبكات الجيل التالي (NGN) أو الفضاء السيبراني. وتركز المبادئ التوجيهية المتعلقة بالأمن على توفير مشورة رسمية بشأن كيفية استخدام آليات أمنية مختلفة لحماية نظام عام لإدارة الهوية كما أنها توفر الإجراءات الأمنية المثلى اللازمة عند التشغيل البيني لنظامين لإدارة الهوية.

التسلسل التاريخي

الصيغة	التوصية	تاريخ الموافقة	لجنة الدراسات
1.0	ITU-T X.1253	2011-09-02	17

تمهيـــد

الاتحاد الدولي للاتصالات وكالة متخصصة للأمم المتحدة في ميدان الاتصالات وتكنولوجيات المعلومات والاتصالات (ICT). وقطاع تقييس الاتصالات (ITU-T) هو هيئة دائمة في الاتحاد الدولي للاتصالات. وهو مسؤول عن دراسة المسائل التقنية والمسائل المتعلقة بالتشغيل والتعريفة، وإصدار التوصيات بشأنها بغرض تقييس الاتصالات على الصعيد العالمي.

وتحدد الجمعية العالمية لتقييس الاتصالات (WTSA) التي تجتمع مرة كل أربع سنوات المواضيع التي يجب أن تدرسها لجان الدراسات التابعة لقطاع تقييس الاتصالات وأن تُصدر توصيات بشأنها.

وتتم الموافقة على هذه التوصيات وفقاً للإجراء الموضح في القرار رقم 1 الصادر عن الجمعية العالمية لتقييس الاتصالات.

وفي بعض مجالات تكنولوجيا المعلومات التي تقع ضمن اختصاص قطاع تقييس الاتصالات، تعد المعايير اللازمة على أساس التعاون مع المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهرتقنية الدولية (IEC).

ملاحظـــة

تستخدم كلمة "الإدارة" في هذه التوصية لتدل بصورة موجزة سواء على إدارة اتصالات أو على وكالة تشغيل معترف بها.

والتقيد بهذه التوصية اختياري. غير أنها قد تضم بعض الأحكام الإلزامية (بهدف تأمين قابلية التشغيل البيني والتطبيق مثلاً). ويعتبر التقيّد بهذه التوصية حاصلاً عندما يتم التقيّد بجميع هذه الأحكام الإلزامية. ويستخدم فعل "يجب" وصيغ ملزمة أخرى مثل فعل "ينبغي" وصيغها النافية للتعبير عن متطلبات معينة، ولا يعني استعمال هذه الصيغ أن التقيّد بهذه التوصية إلزامي.

حقوق الملكية الفكرية

يسترعي الاتحاد الانتباه إلى أن تطبيق هذه التوصية أو تنفيذها قد يستلزم استعمال حق من حقوق الملكية الفكرية. ولا يتخذ الاتحاد أي موقف من القرائن المتعلقة بحقوق الملكية الفكرية أو صلاحيتها أو نطاق تطبيقها سواء طالب بها عضو من أعضاء الاتحاد أو طرف آخر لا تشمله عملية إعداد التوصيات.

وعند الموافقة على هذه التوصية، لم يكن الاتحاد قد تلقى إخطاراً بملكية فكرية تحميها براءات الاختراع يمكن المطالبة بها لتنفيذ هذه التوصية. ومع ذلك، ونظراً إلى أن هذه المعلومات قد لا تكون هي الأحدث، يوصى المسؤولون عن تنفيذ هذه التوصية بالاطلاع على قاعدة المعطيات الخاصة ببراءات الاختراع في مكتب تقييس الاتصالات (TSB) في الموقع http://www.itu.int/ITU-T/ipr/.

جدول المحتويات

الصفحة

التوصيـــة ITU-T X.1253

مبادئ توجيهية بشأن أمن أنظمة إدارة الهوية

1 مجال التطبيق

يشمل مجال تطبيق هذه التوصية ما يلي:

- نماذج وخدمات نظام عام لإدارة الهوية
- التهديدات والمخاطر الأمنية المتصلة بنظام إدارة الهوية
- المبادئ التوجيهية المتعلقة بأمن نشر أنظمة إدارة الهوية
- المبادئ التوجيهية المتعلقة بأمن تشغيل أنظمة إدارة الهوية
- اعتبارات الخصوصية في أنظمة إدارة الهوية

ويركز مجال تطبيق هذه التوصية أساساً على خدمات إدارة الهوية القائمة على ميادين متعددة. ومع ذلك، يمكن تطبيق المبادئ التوجيهية على نظام مركزي لإدارة الهوية.

ملاحظة: يتعين على منفذي ومستعملي المبادئ التوجيهية الموصوفة الالتزام بجميع القوانين واللوائح والسياسات الوطنية والإقليمية المطبقة. وقد تقتضي بعض اللوائح والتشريعات المحددة تنفيذ آليات لحماية المعلومات التي يمكن التعرف على هوية أصحابها شخصياً.

2 المراجع

تشتمل التوصيات والمراجع الأخرى التالية لقطاع تقييس الاتصالات على أحكام تشكّل، من خلال الإشارة إليها في هذا النص، أحكاماً في هذه التوصية. وكانت الطبعات المشار إليها صالحة وقت نشر هذه التوصية. ولما كانت جميع التوصيات والمراجع الأخرى تخضع إلى المراجعة يرجى من جميع المستعملين لهذه التوصية السعي إلى تطبيق أحدث طبعة للتوصيات والمراجع الواردة أدناه. وتنشر بانتظام قائمة توصيات قطاع تقييس الاتصالات سارية الصلاحية. والإشارة إلى وثيقة ما في هذه التوصية لا يضفي على الوثيقة في حد ذاتها صفة التوصية.

[ITU-T X.1205] التوصية ITU-T X.1205 (2008)، *لمحة عامة عن الأمن السيبراني*.

[ITU-T X.1252] التوصية ITU-T X.1252 (2010)، *مصطلحات وتعاريف أساسية تتعلق بإدارة الهوية*.

3 المصطلحات والتعاريف

1.3 مصطلحات معرفة في وثائق أخرى

تستعمل هذه التوصية المصطلحات التالية المعرفة في وثائق أخرى:

1.1.3 التحكم في النفاذ [ITU-T X.1252]: إجراء متبع لتحديد ما إذا كان ينبغي منح كيان ما نفاذاً إلى موارد أو مرافق أو خدمات أو معلومات استناداً إلى ما هو محدد مسبقاً من قواعد وحقوق معينة أو إلى سلطة يتمتع بها الطرف الطالب.

2.1.3 نعت [ITU-T X.1252]: معلومات مرتبطة بكيان تحدد خاصيته.

3.1.3 استيقان (كيان) [ITU-T X.1252]: عملية تستعمل لتحقيق قدر كاف من الثقة في الربط بين الكيان والهوية المقدمة.

4.1.3 أوراق الاعتماد [ITU-T X.1252]: مجموعة بيانات تقدم كدليل على هوية و/أو استحقاقات مزعومة.

5.1.3 هوية [ITU-T X.1252]: تمثيل كيان في شكل واحد أو أكثر من النعوت التي تتيح تمييز الكيان أو الكيانات بالقدر الكافي ضمن سياق. ولأغراض إدارة الهوية (IdM)، يُفهم مصطلح هوية كهوية سياقية (مجموعة فرعية من النعوت)، أي تُحَدّ المجموعة المتنوعة من النعوت بإطار ذي حدود محددة (سياق) يوجد فيه الكيان ويتفاعل.

ملاحظة – يُمثَّل كل كيان بهوية واحدة شاملة تضم جميع عناصر المعلومات المحتملة التي تميز ذلك الكيان (النعوت). بيد أن هذه الهوية الشاملة هي قضية نظرية عصية على أي وصف واستعمال عملي لأن العدد الكلي لجميع النعوت المحتملة لا حصر له.

6.1.3 إدارة الهوية [ITU-T X.1252]: مجموعة من الوظائف والمقدرات (مثل عمليات الإدارة والصيانة والكشف وتبادل الاتصالات والربط والإسناد وإنفاذ السياسة والاستيقان والمزاعم) التي تستعمل من أجل:

- ضمان معلومات الهوية (من قبيل المعرفات والإثباتات والنعوت)؛
- ضمان هوية كيان (مثلاً، مستعملون/مشتركون، مجموعات، أجهزة المستعمل، منظمات، مقدمو الشبكات والخدمات، عناصر وأشياء الشبكة، أشياء افتراضية)؛
- دعم تطبيقات الأعمال التجارية والأمن.

7.1.3 مستعمِل [ITU-T X.1252]: أي كيان يستفيد من مورد، مثل نظام أو معدات أو مطراف أو تطبيق أو شبكة مشاع.

8.1.3 نظام متمحور حول المستعمل [ITU-T X.1252]: نظام إدارة هوية (IdM) يوفر للمستعمل القدرة على التحكم في، وإنفاذ، مختلف سياسات الخصوصية والأمن الناظمة لتبادل معلومات الهوية بين الكيانات، بما فيها معلومات قابلة للتعرّف الشخصي (PII).

2.3 مصطلحات معرفة في هذه التوصية

تعرف هذه التوصية المصطلحات التالية:

1.2.3 كيان: شيء له وجود قائم بذاته ومميز ويمكن تعريفه في سياق.

ملاحظة – يمكن أن يكون الكيان شخصاً طبيعياً أو حيواناً أو شخصاً اعتبارياً أو منظمة، أو شيئاً فاعلاً أو منفعلاً، أو جهازاً، أو تطبيقاً برمجياً، أو خدمة وما إلى ذلك، أو مجموعة مما تقدم. وفي سياق الاتصالات، تشمل أمثلة الكيانات نقاط نفاذ ومشتركين وعناصر شبكة وشبكات وتطبيقات برمجيات وخدمات وأجهزة وسطوح بينية، وما إلى ذلك.

2.2.3 عميل IdM: برنامج عميل يتفاعل مع مخدم IdM لاستخراج معلومات الهوية.

3.2.3 مخدم IdM: المخدم الذي يدير دورة حياة هوية المستعمل.

4.2.3 عميل IdM متنقل: عميل إدارة هوية مثبت ومستخدم في جهاز متنقل.

4 المختصرات والأسماء المختصرة

تستعمل هذه التوصية المختصرات والأسماء المختصرة التالية:

DB قاعدة بيانات *(Database)*

DoS رفض الخدمة *(Denial of Service)*

FDDI السطح البيني للبيانات الموزعة بالألياف البصرية *(Fibre Distributed Data Interface)*

IdM إدارة الهوية *(Identity Management)*

IdP مورد الهوية *(Identity Provider)*

IDS نظام كشف التطفل *(Intrusion Detection System)*

IPS نظام منع التطفل *(Intrusion Prevention System)*

LAN شبكة محلية *(Local Area Network)*

NGN شبكة الجيل التالي *(Next Generation Network)*

OS نظام التشغيل *(Operating System)*

PII معلومات يمكن التعرف على هوية أصحابها شخصياً *(Personally Identifiable Information)*

PIN رقم تعريف الهوية الشخصي *(Personal Identification Number)*

PKI البنية التحتية للمفاتيح العمومية *(Public Key Infrastructure)*

SP مورد خدمة *(Service Provider)*

SSL طبقة مقبس آمنة *(Secure Socket Layer)*

TTP طرف ثالث موثوق *(Trusted Third Party)*

VPN شبكة خاصة افتراضية *(Virtual Private Network)*

5 الاصطلاحات

لا توجد.

6 معلومات أساسية

تطور نظام إدارة الهوية (IdM) على مدى العقد الماضي من نظام منفرد مستقل إلى نظام اتحادي أو متمحور حول المستعمل. وقد ركزت معظم أنظمة تعرف الهوية المستنبطة حتى الآن على كيفية تقديم الخدمات ذات الصلة بالهوية بطريقة فعالة وسهلة. وقد عملت أنظمة كثيرة من أنظمة إدارة الهوية التي طُورت مؤخراً إلى حد ما على توفير الأمن والخصوصية.

في البداية كان نظام إدارة الهوية المعروف بالنموذج المنفرد المستقبل يُنشر في ميدان المؤسسة. وفي هذه الحالة لم تكن هناك أي صلة بين أنظمة إدارة الهوية بحيث لم يكن من الممكن تبادل المعلومات المتعلقة بهوية المستعمل لتوفير بعض الخدمات المفيدة بين الميادين. وعلاوة على ذلك، كان من الممكن تكرار هوية المستعمل الواحد في عدة أنظمة مختلفة لإدارة الهوية. وهذا يجعل من الصعب على إدارة النظام في منظمة ما أن تدير هوية المستعمل بطريقة آمنة وفعالة.

وتمثلت الخطوة التالية في جمع هويات المستعملين في نظام واحد لإدارة الهوية ونشره كلما دعت الحاجة إلى ذلك. وعُرف هذا النهج بالنموذج المركزي. وفي هذا النموذج، يجري جمع معلومات كثيرة جداً بشأن المستعمل في مخدم واحد. وهذا النهج له عدة عيوب نظراً لأن مورد الهوية لا يصبح نقطة اختراق وحيدة فحسب بل قد لا يحظى بثقة جميع الأطراف أيضاً.

ويتمثل النهج التالي في السماح لكل مورد هوية بإدارة هويته وإضفاء الطابع اللامركزي على مسؤوليته من خلال تفويضها لموردين متعددين يمكن أن يختارهم المستعمل. وأصبح هذا النهج يعرف بالنهج الاتحادي. وفي هذا النموذج، يوجد العديد من موردي الهوية الذين يمكن أن يكونوا موضع ثقة لدى المستعمل وأن يديروا معلومات الهوية الخاصة بالمستعملين جزئياً عند اللزوم. ويمكن تبادل معلومات الهوية للمستعمل التي يملكها كل مورد هوية باستعمال جزء من اسم مستعار يدعى هوية اتحادية. ويسمح هذا النموذج بتفادي مشكلة نقطة الاختراق الوحيدة.

ونظراً لأن القضايا المتعلقة بالخصوصية أصبحت متزايدة الأهمية بالنسبة إلى المستعمل، فإن تكنولوجيا إدارة الهوية ركزت على المستعملين لمنحهم كامل السيطرة على معلومات الهوية الخاصة بهم. ويعرف هذا النموذج بالنموذج المتمحور حول المستعمل. ووفقاً لهذا النموذج، يجب أن تمر معلومات الهوية من خلال المستعمل لكي يتسنى له تطبيق سياسة الخصوصية الخاصة به عندما يتبادل موردان للهوية معلومات الهوية المتعلقة بالمستعمل. وقد تمت مواءمة هذا النموذج من خلال العديد من المنتجات الخاصة بالصناعة وهو يضم تكنولوجيات أخرى قائمة لإدارة الهوية.

ويواجه تقارب أنظمة إدارة الهوية هذه مهمة صعبة في كثير من الأحيان فيما يتعلق بكيفية ضمان أمن النظام الناتج عن التقارب وتحقيق التوازن بين الأمن والخصوصية لتوفير الأداء الأمثل. وبالإضافة إلى ذلك، فإن معظم المبادئ التوجيهية المتعلقة بالأمن المقدمة حتى الآن تركز عادة على موردي الهوية والأطراف المعوِّلة على الهوية. ونظراً لأن جوانب الأمن والخصوصية المتعلقة بالمستعمل أصبحت من المتطلبات الإلزامية، من الضروري النظر في الجزء المتمحور حول المستعمل لأمن أنظمة إدارة الهوية من أجل إبراز المخاوف المتزايدة بشأن خصوصية المستعمل.

7 نظرة شاملة عن نظام إدارة الهوية

1.7 نموذج عام لنظام إدارة الهوية

1.1.7 نظام إدارة الهوية المتمحور حول التطبيق

في أنظمة إدارة الهوية الكبيرة، يعني نظام إدارة الهوية المتمحور حول التطبيق أن خدمات وسياسات الهوية مصممة لتلبية احتياجات موردي الهوية والأطراف المعوِّلة وأنها مستمثلة للاستجابة لمتطلبات التطبيقات، مثلاً توفير معلومات تتعلق بحساب المستعمل. وفي نظام إدارة الهوية المتمحور حول التطبيق هناك مورد للهوية وطرف معول. وعند توفير خدمة الهوية للمستعمل، يتم عادة تبادل الهوية بين هذين الكيانين. وتاريخياً، كانت تكنولوجيات إدارة الهوية والنفاذ تُركز أساساً على الاستيقان من المستعملين النهائيين للسماح بنفاذ اتحادي إلى التطبيقات والخدمات. وبالتالي، تقتصر متطلبات الأمن على محيط ميادين التطبيق المعنية.

2.1.7 أنظمة إدارة الهوية المتمحورة حول المستعمل

تركز أنظمة إدارة الهوية المتمحورة حول المستعمل أساساً على المستعملين النهائيين وتُستمثل لتلبية احتياجاتهم. وهذا يعني أن الهدف الرئيسي لنظام إدارة الهوية هو تزويد المستعملين بخدمات هوية مناسبة وشاملة. وتتمثل أهم خاصية لهذا النظام في السماح للمستعمل بالسيطرة الكاملة على هويته. وعند نشر معلومات الهوية الخاصة بالمستعمل، يجب أن تمر عبر المستعمل صراحة لكي يتسنى له تطبيق سياسة شخصية ما إذا لزم الأمر. وفي نظام إدارة الهوية المتمحور حول المستعمل، يجب تثبيت برنامج عميل في البيئة الحاسوبية للمستعمل. ولذلك، هناك حاجة إلى مبادئ توجيهية بسيطة وشاملة لتوجيه المستعمل عند تثبيت البرمجية ذات الصلة ونشرها بطريقة آمنة. ويجب أن تقوم البرمجية بإدارة بعض المعلومات المتعلقة بأمن المستعمل.

وتتميز الأنظمة المتمحورة حول المستعمل عن الأنماط الأخرى لأنظمة إدارة الهوية من حيث إنها تركّز على كون المستعمل، وليس أي هيئة أخرى، هو الذي يتحكم في استحداث نعوت الهوية ونشرها وتحديثها وإلغائها. وهذا يعني أن المستعمل يتمتع بكامل السلطة فيما يتعلق بدورة حياة هويته. ويمكن تحديد مستوى التحكم من خلال احتياجات الخصوصية للمستعمل.

2.7 خدمات الهوية

1.2.7 إدارة دورة حياة الهوية

تقوم هذه الخدمة بإدارة الهوية المستحدثة ونشرها وتحديثها وإلغائها. وتُخزن البيانات المتصلة بهذه الخدمة في قاعدة بيانات توجد في مخدم أو في آلة محلية. وبالتالي، يقتصر النفاذ إلى قاعدة البيانات هذه على المستعملين المخولين.

2.2.7 الاستيقان

تتمثل خدمة الاستيقان في التحقق من هوية المستعملين أو الكيانات الشرعية التي تطلب النفاذ إلى النظام أو الموارد. ويعد الاستيقان الخدمة الرئيسية التي تقدمها أنظمة إدارة الهوية للأطراف المعوِّلة. وينبغي منع قرصنة كلمات السر وانتحال الهوية أياً كان الثمن.

3.2.7 التخويل

ترمي خدمة التخويل إلى معالجة اتخاذ القرارات المتعلقة بحقوق المستعمل من حيث النفاذ وتطبيق القرارات في مجال التخويل وفقاً لامتيازات المستعمل. وهذه الخدمة ضرورية لحماية نظام الهوية من النفاذ والاستعمال غير المرخص بهما.

4.2.7 تبادل النعوت

تؤمن هذه الخدمة تبادل النعوت وتزامنها. وهي واحدة من أهم الخدمات المتعلقة بالأمن علماً أن تبادل النعوت يتم بواسطة شبكة الاتصالات. ويحتاج الأمر إلى مستويات مختلفة من الآليات الأمنية مع تغير وسائط الاتصالات من سلكية إلى لا سلكية.

5.2.7 إذنة الأمن

تعتبر خدمة إذنة الأمن ضرورية لتبادل معلومات الأمن أو الهوية بين الكيانات. وتكون إذنة الأمن محمية بصورة عامة بآليات الأمن والتشفير لأنها تتضمن دائماً معلومات عالية السرية ينبغي ألا يُفصح عنها.

8 التهديدات الأمنية في أنظمة إدارة الهوية

يُفترض أن معظم التهديدات الأمنية التي يتعرض لها الفضاء السيبراني تتعرض لها أنظمة إدارة الهوية أيضاً نظراً لأنها تعمل في الفضاء السيبراني. وتصف التوصية [ITU-T X.1205] التهديدات الأمنية العامة التي يتعرض لها الفضاء السيبراني.

وفي أنظمة إدارة الهوية هناك تهديدات أمنية مختلفة تؤدي إلى إضعاف الأنظمة أو تعرض أمنها للخطر بحيث تصبح المنظمة في خطر كبير.

1.8 أمن الأنظمة

يتمثل أمن الأنظمة بصفة عامة في حماية الأجهزة والبيانات الخاصة بالمستعمل. والهدف هو أن يقتصر النفاذ إلى الأجهزة على المستعملين المخولين فقط وللأغراض المعدة لها من أصحابها. وعلاوة على ذلك، ينبغي استعمال النظام لهذه الأغراض. ويجب ألا يتمكن المهاجمون من تجريد المستعملين الشرعيين من الموارد.

1.1.8 النفاذ والاستعمال غير المرخص بهما

ينبغي ألا يتمكن المستعملون غير المخولين من النفاذ إلى معظم الأنظمة. وينبغي أن تكون أنظمة إدارة الهوية في غاية الصرامة لمنع هذا النوع من التهديدات الأمنية حيث إن النفاذ غير المرخص إلى هوية مخزنة في نظام إدارة الهوية يمكن أن يؤدي إلى المزيد من التهديدات الأمنية من قبيل سرقة الهوية وانتحالها.

2.1.8 الاستعمال غير الملائم

يدل الاستعمال غير الملائم على أنه يمكن لمستعمل ما استخدام نظام إدارة الهوية لإنجاز أو القيام بمهمة معينة لم يُصمم النظام أصلاً من أجلها. وينبغي وجود بعض التقييدات على استخدام أي مستعمل مخول لأجزاء من نظام إدارة الهوية من دون الامتيازات المناسبة. وتكون بعض الخدمات مقتصرة على المستعملين المخولين وبعضها على مستعملين محددين وتكون بعض الخدمات الأخرى محظورة على الجميع باستثناء المدراء.

3.1.8 رفض الخدمة

يمثل نظام إدارة الهوية بصورة عامة نقطة النفاذ الأولى لمستعمل يرغب في استعمال خدمات التطبيق. ولذلك، من المرجح جداً أن تكون أنظمة إدارة الهوية هدفاً للهجوم الذي يهدف إلى وقف توفير الخدمة. وهناك طائفة متنوعة وكبيرة من الهجمات المحتملة لدفع أنظمة إدارة الهوية إلى رفض الخدمة. وغالباً ما تكون هجمات رفض الخدمة سهلة التنفيذ إلى حد كبير ومن الصعب إيقافها. والكثير من هذه الهجمات تهدف إلى استهلاك الموارد الحاسوبية الضخمة مما يجعل من الصعب أو المستحيل خدمة المستعملين الشرعيين.

2.8 التهديدات الأمنية المنفعلة

في سياق التهديدات الأمنية المنفعلة يقرأ المهاجم حزم الشبكة ولكن لا يكتبها. ولعل أبسط طريقة لتنفيذ هجوم من هذا القبيل هو التواجد في نفس الشبكة المحلية التي تتواجد فيها الضحية. وفي معظم التشكيلات المعتادة للشبكة المحلية، بما في ذلك شبكة إثرنت و802.3 وFDDI، يمكن لجميع الآلات الموصلة بالشبكة قراءة إجمالي الحركة الموجهة لأي آلة أخرى في الشبكة المحلية نفسها.

ويتعين إيلاء اهتمام خاص لقنوات الاتصالات اللاسلكية خاصة مع تزايد شعبية الشبكات المحلية اللاسلكية مثل تلك التي تستعمل المعيار 802.11. ونظراً لأن البيانات تُبث على ترددات راديوية معروفة جيداً، فإن المهاجم لا يحتاج إلا إلى وسيلة تمكنه من استقبال هذه الإرسالات. وهذه القنوات معرضة على نحو خاص للهجمات المنفعلة. وعلى الرغم من أن الكثير من هذه القنوات تشمل حماية تقوم على التشفير، فإن هذه التكنولوجيا الأمنية لا تستخدم مع التشكيلة المثلى في أغلب الأحيان.

1.2.8 انتهاك الخصوصية

انتهاك الخصوصية هو انتهاك أي محادثة خصوصية أو اتصال خاص يتم عبر خط الاتصال. وفي حالة الإنترنت، ما زال هناك العديد من الحالات التي تنقل فيها المعلومات السرية بدون تشفير. ويمكن إعادة استخدام أي إثباتات يتم الحصول عليها بواسطة هذا الهجوم لشن المزيد من الهجمات.

2.2.8 التجسس من أجل التعرف على كلمة السر

يتمثل التجسس من أجل التعرف على كلمة السر في الحصول على كلمات سر المستعمل التي تُرسل عبر الشبكة من أجل الحصول على استعمال غير مرخص للموارد. ومن ثم يمكن لمهاجم يستطيع قراءة هذه الحركة التقاط كلمة السر وإعادة استعمالها. وبعبارة أخرى، يمكن للمهاجم أن يبادر إلى التوصيل بنظام إدارة الهوية لسرقة معلومات هوية المستعمل.

3.8 التهديدات الأمنية النشيطة

عندما يشمل الهجوم كتابة البيانات في الشبكة أو في النظام، يشار إلى ذلك بهجوم نشيط. والهجمات النشطة قد تكون عبارة عن تسلل في شبكة حاسوبية بهدف حذف أو تغيير البيانات المخزنة في أنظمة إدارة الهوية التي تشكل جزءاً من الشبكة. وهذا واحد من أخطر أشكال الهجوم نتيجة إلى أن العديد من أنشطة الشركات تعتمد اعتماداً تاماً على هذه البيانات.

1.3.8 هجمات التكرار

في هذه الحالة، يسجل المهاجم سلسلة من الرسائل خارج الشبكة ويعيدها ثانية للطرف المقابل الذي يكون قد استلمها أصلاً. وجدير بالملاحظة أن المهاجم لا يحتاج إلى فهم الرسائل بل إنه بحاجة فقط لالتقاطها وإعادة إرسالها.

2.3.8 هجمات الاعتراض الوسيط

يعترض المهاجم تدفق الاتصال لكي يجعل المرسل يعتقد أنه هو المستقبل ويجعل المستقبل يعتقد أنه هو المرسل. وهذا النوع من الهجوم خطير لأنه يؤدي إلى إخفاء هوية كل من المرسل والمستقبل. ونتيجة لذلك، يمكن أن يكون العديد من التقنيات التي تؤمن سلامة تدفق الاتصال غير كافية للحماية من هجمات الاعتراض الوسيط. وهذا النوع من الهجمات ممكن كلما افتقر البروتوكول إلى استيقان الكيان الند.

4.8 التهديدات الأمنية المتصلة بنظام إدارة الهوية

تتعلق هذه التهديدات بشكل خاص بأنظمة إدارة الهوية. وتمثل التهديدات المذكورة أدناه نقاط الضعف الأمنية الرئيسية التي ينبغي لكل نظام لإدارة الهوية أن يوفر التدابير المضادة المناسبة للتصدي لها.

1.4.8 التهديدات المتصلة بكلمات السر

يعزى أحد التهديدات المرتبطة بكلمات السر إلى استخدام كلمة سر ضعيفة. إذا اختار المستعمل كلمة سر ضعيفة – أي يمكن تخمينها – من أجل الاستيقان، يمكن أن تتعرض كلمة السر لهجوم القاموس. وتحدث مشكلة أخرى عندما يقوم المستعمل باستخدام نفس كلمة السر الضعيفة للتسجيل للدخول إلى مواقع مختلفة على الويب. وفي هذه الحالة، فإن كل موقع ويب تشوبه نقاط ضعف من حيث الأمن يمكن أن يتعرض لهجوم لكشف كلمة السر الخاصة بالمستعمل، وهكذا لا يكون على المهاجم سوى محاولة الدخول إلى مواقع أخرى على الويب باستخدام كلمات السر المسروقة.

ويتمثل التهديد الآخر في التجسس للحصول على كلمة السر بواسطة برامج تجسس تُثبّت في أجهزة الحاسوب. ويمكن لأجهزة الحاسوب أن تصاب ببرامج تجسس قادرة على قرصنة كلمة السر الخاصة بالمستعمل أو مدير الشبكة.

2.4.8 النفاذ غير المخول

النفاذ غير المخول تعبير يشير إلى عدد من مختلف أشكال الهجمات. والهدف النهائي للمهاجم هو الحصول على النفاذ إلى بعض الموارد بصورة غير مشروعة [ITU-T X.1205].

ويجب أن يكون نظام إدارة الهوية الذي يوفر خدمات الاستيقان والهوية متيسراً ومتاحاً لجميع الأطراف التي تحتاج إلى استخدام هوية المستعمل من أجل توفير خدمات التطبيق. ومن ثم، يجب وضع آلية تحكم في النفاذ تكون تفصيلية ودقيقة من أجل حماية النظام من النفاذ غير المرخص به.

3.4.8 التنصت

التنصت تهديد يصعب اكتشافه. فهدف المهاجم هنا هو ترصد البيانات الخام في شبكة المنطقة المحلية للمؤسسة وتسجيلها في الغالب. ويستخدم التنصت "أسلوب الاختلاط" لمكيفات الإثرنت الجاهزة التي تباع في الأسواق. وتتيح هذه الطريقة للمهاجم التقاط كل رزمة على الشبكة. ويوجد حالياً الكثير من كاشفات الشبكات المجانية على الويب التي يمكن أن يستخدمها المهاجم في التنصت [ITU-T X.1205].

وبصورة عامة، تتواصل أنظمة إدارة الهوية مع المستعملين والكيانات الأخرى لتبادل الإثباتات ومعلومات الهوية التي غالباً ما تكون سرية وذلك باستخدام شبكة سلكية أو لا سلكية. ولذلك، فإن أي معلومات يتم التقاطها بواسطة التنصت يمكن أن تؤدي إلى سرقة الهوية.

4.4.8 الاحتيال

محاولة يقوم بها طرف ثالث للحصول على معلومات سرية من أي فرد أو مجموعة أو منظمة عن طريق محاكاة أو انتحال علامة تجارية محددة، تكون عادة معروفة، لتحقيق مكاسب مالية عادة. ويحاول المهاجم خداع المستعملين من خلال دفعهم إلى الكشف عن بيانات شخصية مثل أرقام بطاقات الائتمان والإثباتات المصرفية المستعملة على الخط وغيرها من المعلومات الحساسة التي يمكن أن يستخدمها فيما بعد لارتكاب أفعال احتيالية. والموقع الشبكي للاحتيال هو عبارة عن موقع مصمم لتقليد الموقع الشبكي المشروع للمنظمة التي تتعرض علامتها التجارية للاحتيال. وفي أنظمة إدارة الهوية، يمثل الاحتيال تهديداً خطيراً نظراً لأنه بمجرد استيلاء المهاجم على معلومات استيقان الضحية أو غيرها من المعلومات التي تؤدي إلى التعرف على هوية أصحابها، يمكنه استعمالها في سرقة الهوية أو لارتكاب أعمال احتيالية أخرى.

5.4.8 سرقة الهوية

يتعلق الأمر بمسألة أمنية من الدرجة الأولى، لا سيما للمنظمات التي تقوم بتخزين وإدارة أحجام كبيرة من المعلومات التي يمكن التعرف على هوية أصحابها شخصياً. وهذا النوع من الانتهاك الذي يؤدي إلى فقدان هذه المعلومات لا يقتصر على تقويض ثقة العملاء والمؤسسات وإلحاق الضرر بسمعة المنظمة، وإنما يمكن أن يكون انتهاك البيانات أيضاً مكلفاً مالياً بالنسبة للمنظمات.

9 المبادئ التوجيهية المتعلقة بأمن أنظمة إدارة الهوية

تحدد المبادئ التوجيهية الواردة في الفقرتين 1.9 و2.9 كيفية تأمين نشر وتشغيل نظام عام لإدارة الهوية. وتقدم هذه المبادئ التوجيهية المتطلبات الأمنية الأساسية بشأن نظام لإدارة الهوية يمكن نشره وتشغيله بطريقة آمنة في بيئات حاسوبية مختلفة. وتتناول الفقرات 3.9 و4.9 و5.9 الكيانات التي تتكون منها أنظمة إدارة الهوية وهي مخدم إدارة الهوية وعميل إدارة الهوية والعميل المتنقل لإدارة الهوية. وتقدم الفقرة 6.9 اعتبارات الخصوصية في أنظمة إدارة الهوية.

1.9 المبادئ التوجيهية المتعلقة بأمن نشر أنظمة إدارة الهوية

تقدم هذه الفقرة المبادئ التوجيهية الأمنية اللازمة عند تثبيت نظام إدارة الهوية ونشره. وفي معظم الحالات، يجب اتخاذ الإجراءات اللازمة لضمان إدارة الثقة والمفاتيح.

1.1.9 إدارة الثقة

يعتمد إصدار أي ترخيص باستعمال أنظمة إدارة الهوية على الثقة بأن الهوية ونعوتها أصلية وصحيحة. ولذلك، لا تكون الهوية مفيدة إلا عند اقترانها بمرجع مقنع. وينشأ هذا المرجع على أساس الثقة. وتمثل خطة إدارة الثقة الخطوة الأولى لنشر أنظمة إدارة الهوية وتشغيلها على نحو سليم.

والبنية التحتية للمفاتيح العمومية (PKI) هي إحدى آليات الثقة الأساسية لأنظمة إدارة الهوية. والغرض الرئيسي لهذه البنية التحتية هو توفير شهادة المفتاح العمومي التي يمكن استعمالها من أجل الاستيقان وإنشاء قناة آمنة. وفي أنظمة إدارة الهوية الكبيرة، يوصى بشدة بإنشاء طرف ثالث موثوق (TTP) باستعمال البنية التحتية للمفاتيح العمومية. ويمكن استعمال الشهادة الصادرة عن البنية التحتية للمفاتيح العمومية لاستيقان مستعمل نظام إدارة الهوية وتشفير قناة الاتصال في طبقة المقبس الآمنة (SSL). ويمثل التوقيع الرقمي تطبيقاً رئيسياً آخر للشهادة.

2.1.9 أمن الشبكة

ينبغي تأمين بيئة شبكة الاتصالات باستخدام مختلف الوسائل. وبادئ ذي بدء، ينبغي تأمين محيط الشبكة بواسطة جدار الحماية. وينبغي أن يقع أي نظام لإدارة الهوية داخل محيط جدار الحماية. وبالإضافة إلى ذلك، يمكن استعمال آليات خاصة بأمن الشبكة تكون أكثر تطوراً مثل الشبكات VPN وIDS/IPS لتعزيز أمن بيئات الشبكة.

3.1.9 بيئة الشبكة المضيفة الآمنة

تشير البيئة المضيفة إلى مكان تثبيت نظام إدارة الهوية وتشغيله. وينبغي أن تكون المخدمات أو محطات التشغيل التي يُثبّت فيها مكون نظام إدارة الهوية، مجهزة ببرامج مكافحة الفيروسات وحماية لوحة المفاتيح قبل تثبيت نظام إدارة الهوية. وينبغي التأكد من أن البيئة المضيفة لم تتعرض لأي هجمات تتعلق بالأمن قبل تثبيت نظام إدارة الهوية ونشره.

4.1.9 التخزين الآمن

يُحفظ الكثير من البيانات الهامة والحساسة في وسائط تخزين مثل قاعدة البيانات أو مخدم الدليل. ولدى الإعداد، ينبغي تثبيت مخدم التخزين في جهاز حاسوب آمن وينبغي إنشاء حساب خاص بمدير الشبكة استناداً إلى المبادئ التوجيهية المناسبة للتثبيت لمنع فتح حساب احتيالي واستخدامه فيما بعد لإلحاق الضرر بالنظام.

2.9 المبادئ التوجيهية المتعلقة بأمن تشغيل أنظمة إدارة الهوية

تقدم هذه الفقرة المبادئ التوجيهية المتعلقة بأمن تشغيل نظام إدارة الهوية. ويمثل التحكم في الاستيقان والنفاذ إحدى المسائل الهامة التي ينبغي بحثها.

1.2.9 التوقيع الرقمي

يمثل التوقيع الرقمي آلية الأمن التي يمكن أن تضمن صحة وسلامة الرسالة التي تم توقيعها. وفي نظام إدارة الهوية، هناك العديد من الحالات التي يكون فيها على المستعمل إثبات رغبته أو موافقته على المعاملات الرقمية. وفي هذه الحالة، يمكن أن يكون التوقيع الرقمي المستعمل بمثابة دليل للتحقق من سلامة المعاملة.

2.2.9 التشفير

يحتم نظام إدارة الهوية التشفير عند مختلف مستويات التشغيل. فبداية، يجب تشفير الرسائل المتبادلة بين الكيانات إذا كانت السرية ضرورية. واعتماداً على سياسة تشغيل نظام إدارة الهوية، يجب أن تكون بعض البيانات المخزنة في قاعدة البيانات مشفرة توخياً للسرية ومنع النفاذ غير المرخص به. ويوفر التشفير أقصى قدر من السرية لأنظمة إدارة الهوية ويضمن في نهاية المطاف خصوصية المستعمل ومعلومات الهوية الخاصة به.

3.2.9 الاستيقان

يعتبر الاستيقان بمثابة بوابة لمنع وصول المستعملين غير الشرعيين إلى النظام بدون نفاذ مخول. وفيما يتعلق بشبكة الإنترنت، يستخدم الاستيقان البسيط بواسطة اسم المستخدم/كلمة السر على نطاق واسع ولكنه ينطوي على نقاط ضعف كثيرة من حيث إجراءات الأمن. ولذلك، يوصى باستعمال استيقان قوي كلما لزم ضمان مستوى عالٍ من الثقة في أي مستعمل يحاول النفاذ إلى النظام. ويمكن التقليل من خطر الهجمات المتعلقة بالاحتيال أو الخداع من خلال الاستيقان المتبادل.

4.2.9 الاتصال الآمن

معظم المعلومات المتبادلة بين المستعمل ونظام إدارة الهوية تتعلق بالخصوصية وتكون سرية بطبيعتها. وإضافة إلى ذلك، يمكن أن تتضمن رسائل البروتوكول المتبادلة بين الكيانات معلومات حساسة وسرية يتعين تشفيرها عبر خطوط الاتصالات. ويمكن تأمين الاتصالات باستعمال التقنيات الموجودة مثل الطبقة SSL والشبكة VPN.

5.2.9 التحكم في النفاذ

يمكن لكيانات مختلفة كالمديرين والمستعملين النفاذ إلى نظام إدارة الهوية للحصول على خدمة معنية أو صيانة روتينية. ويجب توفر آلية مناسبة للتحكم في النفاذ من أجل منع أطراف ثالثة مؤذية من التغلغل في النظام. وفي معظم الحالات، يكون نموذج التحكم في النفاذ التمييزي (أي قوائم التحكم في النفاذ) كافياً. ومع ذلك، نظراً لأن نموذج التحكم في النفاذ القائم على الأدوار يمكن أن يوفر تحكماً أكثر دقة وأكثر تطوراً، من الممكن تطبيقه عندما يكون من المطلوب نموذج تحكم أكثر أمناً ومرونة.

3.9 المبادئ التوجيهية المتعلقة بأمن مخدمات إدارة الهوية

تقدم هذه الفقرة مبادئ توجيهية أمنية محددة لمخدمات إدارة الهوية المثبتة والمشغلة في محطات التشغيل أو المخدمات كبيرة الحجم.

1.3.9 تأمين نظام التشغيل

تعمل مخدمات إدارة الهوية الأكثر شيوعاً في نظام تشغيل (OS) مخصص للأغراض عامة. ويمكن تفادي الكثير من المشاكل الأمنية إذا ما تم تشكيل نظام التشغيل الذي يستعمله مخدم نظام إدارة الهوية تشكيلاً مناسباً. وبما أن مخدم إدارة الهوية يثبت في نظام التشغيل القائم، فإن أمنه يعتمد أساساً على أمن نظام التشغيل. وتختلف التقنيات التي تسمح بتأمين أنظمة التشغيل المختلفة اختلافاً كبيراً؛ وبالتالي، تتناول هذه الفقرة الإجراءات العامة المشتركة لتأمين معظم أنظمة التشغيل. ويمكن الاطلاع على المزيد من المعلومات بشأن الإدارة الأمنية الأساسية في نظام التشغيل في التوصية [ITU-T X.1205] والمعيار [b-NIST SP 800-123].

وبغية تأمين مخدمات إدارة الهوية، يجب تأمين نظام التشغيل باتباع الخطوات الأساسية التالية:

- سد الثغرات في نظام التشغيل وتحديثه
- تعزيز وتشكيل نظام التشغيل لضمان الأمن على نحو كافٍ
- تثبيت وتشكيل آليات أخرى للتحكم في الأمن عند اللزوم
- اختبار أمن نظام التشغيل لضمان معالجة الخطوات السابقة لجميع المسائل الأمنية على نحو كافٍ.

2.3.9 تشكيل استيقان المستعمل

بالنسبة لمخدمات إدارة الهوية، ينبغي أن يقتصر تشكيل المخدم على عدد قليل من المستعملين المخولين من مدراء المخدم المعينين. ولفرض القيود المتعلقة بالسياسة إذا لزم الأمر، ينبغي لمدير المخدم أن يقوم بتشكيل المخدم لاستيقان المستعمل من خلال طلب تقديم إثبات أن المستعمل مخول لهذا النفاذ. وفي حالة مخدمات إدارة الهوية التي يجب أن توفر مستويات عالية من الثقة والأمان، يمكن للمنظمات أن تستعمل أيضاً معدات استيقان مقاومة للتزييف، من قبيل الإذنات أو أجهزة تقوم على استخدام كلمة السر مرة واحدة. وفي هذه الحالة، يوصى بشدة بعدم استخدام آليات الاستيقان التي تسمح بإعادة استعمال معلومات الاستيقان (مثلاً، كلمات السر) وإرسالها في شكل نص عادي عبر شبكة غير موثوقة، حيث يمكن للمهاجم اعتراض المعلومات واستعمالها للتنكر في شكل مستعمل مخول.

غالباً ما يشمل التشكيل بالتغيب لنظام التشغيل حسابات للضيوف مع كلمة سر أو بدون. ينبغي لمدير الشبكة إلغاء أو تعطيل حسابات الضيوف غير المستعملة لكي يتعذر على المهاجمين استخدامها.

3.3.9 تشكيل التحكم في النفاذ

يسمح معظم مخدمات إدارة الهوية بتحديد امتيازات النفاذ الخاصة بكل إثبات أو معلومة من معلومات الهوية. وكل مستعمل ينفذ إلى مخدم إدارة الهوية ينبغي ألا يكون مخولاً للنفاذ إلى معلومات الهوية الخاصة بمستعملين آخرين. ويمكن للإعداد الصحيح لعناصر التحكم في النفاذ أن يساعد في منع إفشاء معلومات الهوية الحساسة أو المقيدة التي ليست معدة للنشر العام. وبالإضافة إلى ذلك، يمكن استخدام عناصر التحكم في النفاذ للحد من استعمال الموارد في حالة وقوع هجوم ضد المخدم من هجمات رفض الخدمة (DoS).

4.3.9 التسجيل

يعد التسجيل جزءاً أساسياً من التدابير المضادة الفعالة في مجال الأمن. ومن المهم جداً التقاط البيانات الصحيحة وإدراجها في السجلات التي يتم رصدها عن كثب فيما بعد. وتعد سجلات الشبكات والأنظمة مهمة لا سيما سجلات الأنظمة في حالة الاتصالات المشفرة في حين يكون رصد الشبكات أقل فعالية.

ومراجعة السجلات طريقة إلزامية وفعالة للبحث عن أي نشاط مشبوه. ففي كثير من الحالات، غالباً ما تكون ملفات السجل الدليل الوحيد على سلوك مشبوه. ويتيح تمكين الآليات من تسجيل المعلومات باستعمال السجلات للكشف عن محاولات التسلل الفاشلة أو الناجحة واستهلال آليات الإنذار عند الحاجة إلى المزيد من التحريات. وثمة حاجة إلى وضع إجراءات وأدوات لمعالجة وتحليل ملفات السجلات وتحليلها ومراجعة تبليغات الإنذار.

وينبغي ضمان قدرة عناصر التحكم في النفاذ على فصل المهام من خلال ضمان عدم إمكانية تعديل سجلات المخدم من طرف مديري المخدم وضمان، إن أمكن، أن يكون المخدم مخولاً فقط بحيث يُلحق بملفات السجلات.

4.9 المبادئ التوجيهية الأمنية المتعلقة بعملاء إدارة الهوية

تقدم هذه الفقرة المبادئ التوجيهية الأمنية لدى تشغيل أحد البرامج الخاصة بعميل إدارة الهوية. وفي حال استخدام متصفح الويب كعميل إدارة الهوية، تكون مواطن الضعف المتعلقة بالأمن متوقفة على المتصفح ذاته. ومع ذلك ما زالت هناك بعض المبادئ التوجيهية الأمنية التي يمكن اتباعها لضمان أمن بيئة العميل.

1.4.9 التوزيع الآمن لبرنامج العميل

في الوقت الحالي يتم تنزيل معظم البرامج المساعدة المرتبطة بالمتصفح من أحد مواقع الويب. وإذا قام مستعمل عن طريق الخطأ بتنزيل برنامج عميل لإدارة الهوية يمكن أن يلحق الضرر بنظامه، فإنه لا توجد آلية أمنية قوية يمكنها حماية المستعمل من الأنشطة الخبيثة. ولذلك يجب أن يكفل موردو برامج عميل إدارة الهوية سلامة البرنامج الموزع وأن هذا البرنامج يوفر طريقة آمنة للتحقق من سلامته.

2.4.9 سلامة برنامج عميل إدارة الهوية

يمثل التوقيع الرقمي واحداً من أفضل الحلول لكفالة سلامة برنامج عميل معين. وإذا كان برنامج العميل موقعاً من أحد موردي الخدمة وتم تقديم شهادة توقيع للتحقق، يمكن للمستعمل تنزيل البرنامج بشكل آمن والتحقق من سلامة شفرة البرنامج. وهناك طريقة بديلة تقوم على استعمال خوارزمية التجزئة لضمان سلامة الشفرة. وشفرة العميل هو المدخل الذي تستخدمه الخوارزمية لإنتاج قيمة التجزئة التي هي خلاصة شفرة العميل. وإذا نشرت قيمة التجزئة على الويب بطريقة آمنة، يمكن للمستعمل التحقق من صحة البرنامج العميل من خلال حساب قيمة التجزئة للبرنامج الذي تم تنزيله. ومع ذلك تعتبر الطريقة الأولى أكثر أمناً من الطريقة الثانية.

3.4.9 ملف قاعدة بيانات البرنامج العميل

يجب تخزين ملفات قاعدة البيانات (DB) الخاصة ببرنامج العميل بطريقة آمنة. وينبغي أن يقتصر النفاذ إلى قاعدة البيانات هذه على مستعملين مستيقن منهم. وفي معظم الحالات، يقوم العميل IdM بإدارة المعلومات المتعلقة بإثباتات المستعمل بما في ذلك كلمات السر وإذنات الأمن التي ينبغي الاحتفاظ بها في شكل مشفر لضمان السرية. وينبغي أيضاً حماية ملفات قاعدة البيانات ذاتها من التغير أو التعديل غير المشروعين لكفالة سلامتها. وعند إلغاء ملف من ملفات قاعدة البيانات من نظام ما، ينبغي ألا يُترك أي أثر على القرص الصلب يسمح باسترجاع البيانات لاحقاً.

4.4.9 كلمة السر الآمنة

تعتمد معظم آليات الأمن بصورة أساسية على كلمة سر تسمح بالاستيقان للنفاذ إلى النظام. فإذا اختار المستعمل كلمة سر ضعيفة يمكن خرقها بهجوم قوي، ولا يمكن بعدها لأي آلية أمن أخرى أن تحمي النظام من المستعملين ذوي النوايا السيئة. وبالتالي، تتمثل أهم مهمة لمورد خدمة إدارة الهوية في ضمان اختيار المستعمل لكلمة سر قوية للدخول إلى النظام.

5.4.9 إلغاء تثبيت برنامج عميل

عند إلغاء تثبيت برنامج عميل في نظام معين، ينبغي حذف جميع كلمات السر والإثباتات ومعلومات الهوية بصورة دائمة كما ينبغي حذف التشكيلة الشخصية لبرنامج العميل.

5.9 المبادئ التوجيهية المتعلقة بأمن عميل متنقل لإدارة الهوية

تقدم هذه الفقرة المبادئ التوجيهية المتعلقة بأمن عملاء متنقلين لإدارة الهوية مثبتين ومشغلين في جهاز متنقل. ويتميز الجهاز المتنقل بخصائص محددة مثل قابلية الحمل والتنقل. ومع ذلك يمكن أن تشكل هذه الخصائص نقاط ضعف على مستوى الأمن إذا ما حاول المهاجم استغلالها.

1.5.9 ضياع الجهاز أو سرقته

بما أن الأجهزة المتنقلة قابلة للحمل، من المحتمل جداً أن تضيع أو تتعرض للسرقة. وهناك العديد من الطرق للتسلل إلى جهاز متنقل لاستخراج المعلومات الشخصية من أجل انتحال الهوية. ولذلك ينبغي أن يكون العميل المتنقل المثبت داخل الجهاز معداً لمواجهة أي هجوم أمني قد يتسبب في استعمال غير مرخص أو انتحال الهوية. وعندما يضيع الجهاز أو يتعرض للسرقة، يتم الإبلاغ عن الحادث إلى مورد خدمة الاتصالات المتنقلة وبناءً على الحالة، يمكن للمشغل أن يقوم بإغلاق الجهاز عن بعد لمنع أي نفاذ إليه. ويكون هذا الإجراء مناسباً عندما يضيع الجهاز في بيئة لا تشوبها المخاطر مثل المنزل أو مكان العمل. وفي جميع الحالات الأخرى، ينبغي أن يكون المشغل قادراً على حذف جميع المعلومات الشخصية أو سجلات الهوية المخزنة في الجهاز إذا تأكد صاحب الجهاز أنه فقد الجهاز أو سُرق منه نهائياً وليس هناك من طريقة لاسترجاعه.

2.5.9 استيقان الجهاز

إذا كان الجهاز المحمول مجهزاً بشاشة صغيرة الحجم، فإنه من الصعب جداً الدخول إلى الجهاز باستخدام كلمة سر قائمة على الأبجدية الرقمية في كل مرة يتم فيها استخدام الجهاز. وفي هذه الحالة يُستعمل رقم تعريف الهوية الشخصي (PIN) ككلمة سر، ولكن لا يستعمل هذا الأمر في العديد من الحالات لأغراض التيسير. وللتغلب على هذا الوضع، ينبغي أن يوفر العميل المتنقل لإدارة الهوية آليات استيقان سهلة للمستعمل ولكن آمنة بما يكفي ومناسبة للجهاز المتنقل. ويتعين على العميل المتنقل تنفيذ الاستيقان بواسطة كلمة السر في حال كان الجهاز لا يستعمل أي آلية استيقان لدخول المستعمل إلى النظام.

3.5.9 الحماية الاحتياطية لقاعدة البيانات

يتم تجميع معظم معلومات الهوية ومعالجتها داخل الجهاز المتنقل من أجل خدمات مختلفة. غير أن العديد من تلك الهويات هي معلومات شخصية حساسة ومرتبطة بالخصوصية تلزم حمايتها من أجل السلامة والسرية. وكما ذكر سابقاً، فإن الأجهزة المتنقلة معرضة بسهولة للضياع والسرقة. ولذلك فإن العميل المتنقل لإدارة الهوية بحاجة إلى توفير طريقة لإعداد نسخ احتياطية

لقاعدة البيانات الخاصة بمعلومات الهوية. ويمكن القيام بذلك بطريقتين. تتمثل الطريقة الأولى في القيام بإعداد نسخ احتياطية لقاعدة البيانات في وسط تخزين ثانوي مثل بطاقة الذاكرة الرقمية الآمنة (SD) إذا كانت متوفرة. وتتمثل الطريقة الثانية في استعمال مخدم تأمين خارجي لتوفير خدمة إعداد نسخة احتياطية لقاعدة البيانات الخاصة بالعميل. وفي هذه الحالة، يمكن عادةً استرجاع قاعدة بيانات المستعمل حتى في حالة ضياع الجهاز أو سرقته.

4.5.9 أمن الاتصالات المتنقلة

تستعمل الأجهزة المتنقلة الاتصالات المتنقلة من أجل التواصل فيما بينها في معظم الأحيان. ومع ذلك من المعترف به أن الاتصالات المتنقلة معرضة بشكل كبير إلى الهجمات النشيطة أو المنفعلة. ويرسل العميل المتنقل لإدارة الهوية معلومات شخصية حساسة عبر الوصلة المتنقلة. ومن ثم فإن سلامة وسرية أي اتصال مع العميل المتنقل عبر الوصلات المتنقلة يحتاج إلى الحماية بواسطة آلية أمن متاحة في طبقة النقل.

6.9 اعتبارات الخصوصية في أنظمة إدارة الهوية

تعد الخصوصية مسألة بالغة الأهمية في سياق أمن إدارة الهوية. ومع ذلك يوجد العديد من القواعد واللوائح الخاصة بكل بلد على حدة عندما يتعلق الأمر بتطبيق المبادئ التوجيهية من الناحية العملية. ومن ثم، تبحث هذه الفقرة بعض المسائل المتعلقة بالخصوصية في سياق أنظمة إدارة الهوية وتقدم هذه المسائل على سبيل العلم.

1.6.9 موافقة المستعمل

عندما تُجمّع معلومات الهوية من المستعمل ويتم استعمالها من جانب مورد هوية أو مورد خدمة، يجب الحصول على موافقة المستعمل صراحة. ويكون من الأفضل الحصول على موافقة المستعمل بشكل من أشكال التوقيع الرقمي الذي يمكن التحقق منه فيما بعد إذا استدعى الأمر.

2.6.9 اختيار الهوية

تزود أنظمة إدارة الهوية المستعمل صراحة بإمكانية اختيار ما إذا كان يسمح بجمع المعلومات المتعلقة بهويته ونقلها واستعمالها وتخزينها وأرشفتها والتخلص منها. وتتعزز خصوصية المستعمل نظراً لأنه هو الذي يتحكم في إدارة سياسة الهوية والخصوصية. وينبغي مراعاة هذا النهج المتمحور حول المستعمل لدى تصميم نظام إدارة الهوية.

3.6.9 الغرض من الهوية

ينبغي لنظام إدارة الهوية أن يبين للمستعمل جميع الأغراض التي تُجمع من أجلها المعلومات الشخصية وتُستعمل، وينبغي أن يتم ذلك بطريقة يسهل فهمها وقبل جمع المعلومات المتعلقة بهويته. كما ينبغي للنظام بذل كافة الجهود الممكنة لاستعمال الهوية في الغرض المحدد.

4.6.9 الحد من الهويات وتقليلها إلى أدنى حد

ينبغي لأنظمة إدارة الهوية التي تقوم بجمع الهويات أن تجمع فقط الهويات اللازمة لتحقيق الأهداف المحددة، ما لم تكن هناك موافقة من الفرد أو بناءً على ما هو مسموح به أو مطلوب بموجب القانون.

وينبغي لنظام إدارة الهوية الذي يقوم بجمع الهويات أن ينظر بدقة ويوثق الإجراءات التي تبين بوضوح الهوية اللازمة ولأي غرض وكيفية ضمان أن جميع عمليات معالجة الهوية تتعلق فقط بتجميع الحد الأدنى من الهويات اللازمة للأغراض الخاصة بها.

5.6.9 إلغاء الهوية

ينبغي لأنظمة إدارة الهوية أن تلغي الهوية بعد أن يتم تحقيق الهدف المنشود و لم تكن هناك التزامات قانونية أو تنظيمية تقتضي مدة بقاء أطول. وعند إلغاء الهوية، ينبغي أيضاً التأكد من إلغاء جميع المعلومات المتعلقة بالهوية المخزنة في الأنظمة ذات الصلة مثل نظامي النسخ الاحتياطي والأرشيف.

6.6.9 إعداد سياسة الخصوصية

قبل تشغيل نظام إدارة الهوية، يمكن تحديد سياسات الخصوصية مثل تفضيلات الخصوصية وسياسات تخويل الخصوصية. وتحكم هذه السياسة استخدام الهوية التي يقدمها المستعمل إلى النظام.

7.6.9 إغفال الهوية

يمكن أن يمثل إغفال الهوية الهدف النهائي المتوخى تحقيقه في نظام لإدارة الهوية يحقق خصوصية معززة. ومع ذلك، فإن اقتراح تكلفة معقولة مهمة صعبة ومعقدة للغاية. وبالتالي، يمكن في معظم الحالات استعمال اسم مستعار للوفاء بمتطلبات الخصوصية لنظام إدارة الهوية.

بيبليوغرافيا

[b-NIST SP 800-123] Scarfone, K.A., Jansen, W., and Miles, T. (2008), *Guide to General Server Security*, NIST Special Publication SP-800-123.

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة D	المبادئ العامة للتعريفة
السلسلة E	التشغيل العام للشبكة والخدمة الهاتفية وتشغيل الخدمات والعوامل البشرية
السلسلة F	خدمات الاتصالات غير الهاتفية
السلسلة G	أنظمة الإرسال ووسائطه والأنظمة والشبكات الرقمية
السلسلة H	الأنظمة السمعية المرئية والأنظمة متعددة الوسائط
السلسلة I	الشبكة الرقمية متكاملة الخدمات
السلسلة J	الشبكات الكبلية وإرسال إشارات تلفزيونية وبرامج صوتية وإشارات أخرى متعددة الوسائط
السلسلة K	الحماية من التداخلات
السلسلة L	إنشاء الكبلات وغيرها من عناصر المنشآت الخارجية وتركيبها وحمايتها
السلسلة M	إدارة الاتصالات بما في ذلك شبكة إدارة الاتصالات (TMN) وصيانة الشبكات
السلسلة N	الصيانة: الدارات الدولية لإرسال البرامج الإذاعية الصوتية والتلفزيونية
السلسلة O	مواصفات تجهيزات القياس
السلسلة P	نوعية الإرسال الهاتفي والمنشآت الهاتفية وشبكات الخطوط المحلية
السلسلة Q	التبديل والتشوير
السلسلة R	الإرسال البرقي
السلسلة S	التجهيزات المطرافية للخدمات البرقية
السلسلة T	المطاريف الخاصة بالخدمات التلماتية
السلسلة U	التبديل البرقي
السلسلة V	اتصالات البيانات على الشبكة الهاتفية
السلسلة X	**شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن**
السلسلة Y	البنية التحتية العالمية للمعلومات وملامح بروتوكول الإنترنت وشبكات الجيل التالي
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات

طُبعت في سويسرا
جنيف، 2012